A Lecture on Quantum Logic Gates

Kazuyuki FUJII*

Department of Mathematical Sciences

Yokohama City University

Yokohama, 236-0027

Japan

Abstract

In this note we make a short review of constructions of n-repeated controlled unitary gates in quantum logic gates.

*E-mail address : fujii@math.yokohama-cu.ac.jp

1 Introduction

This is one of my lectuers entitled "Introduction to Quantum Computation" given at Graduate School of Yokohama City University. The contents of lecture are based on the book [1] and review papers [2], [3]. The controlled NOT gate (more generally, controlled unitary gates) plays very important role in quantum logic gates to prove a universality. The constructions of controlled unitary gates or controlled-controlled unitary gates are clear and easy to understand. But the construction of general controlled unitary gates (n-repeated controlled unitary gates) seem, in my teaching experience, not easy to understand for young graduate students. I thought out some method to make the proof more accessible to them. I will introduce it in this note. Maybe it is, more or less, well-known in some field in Pure Mathematics, but we are too busy to study such a field leisurely. I believe that this note will make non-experts more accessible to quantum logic gates.

2 Some Identity on Z_2

Let us start with the mod 2 operation in Z_2 : for $x, y \in Z_2$

$$x \oplus y = x + y \ (\mathrm{mod}2). \tag{1}$$

From the relations

$$0 \oplus 0 = 0,\ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0,$$

it is easy to see

$$x \oplus y = x + y - 2xy, \ \text{or} \quad x + y - x \oplus y = 2xy. \tag{2}$$

We note that $x \oplus 0 = x,\ x \oplus 1 = 1 - x,\ x \oplus x = 2x - 2x^2 = 2x(1-x) = 0.$

From $x + y - x \oplus y = 2xy$ we have

$$x + y + z - (x \oplus y + x \oplus z + y \oplus z) + x \oplus y \oplus z = 4xyz \tag{3}$$

for $x, y, z \in Z_2$. The proof is easy, so we leave it to the readers. Moreover we have

$$\begin{aligned} & x+y+z+w-(x\oplus y+x\oplus z+x\oplus w+y\oplus z+y\oplus w+z\oplus w)+(x\oplus y\oplus z+ \\ & x\oplus y\oplus w+x\oplus z\oplus w+y\oplus z\oplus w)-x\oplus y\oplus z\oplus w=8xyzw \end{aligned} \tag{4}$$

for $x, y, z, w \in Z_2$. But is this proof so easy ?

Now we define a function

$$\begin{aligned} F_n(x_1,\cdots,x_n) &= \sum_{i=1}^{n} x_i - \sum_{i<j}^{n} x_i\oplus x_j + \sum_{i<j<k}^{n} x_i\oplus x_j\oplus x_k - \cdots \\ &+ (-1)^{n-2}\sum_{i=1}^{n} x_1\oplus\cdots\oplus\breve{x}_i\oplus\cdots\oplus x_n + (-1)^{n-1}x_1\oplus\cdots\oplus x_n \end{aligned} \tag{5}$$

for $x_1, \cdots, x_n \in Z_2$. From (2), (3) and (4) we have $F_2(x_1, x_2) = 2x_1x_2$ and $F_3(x_1, x_2, x_3) = 4x_1x_2x_3$ and $F_4(x_1, x_2, x_3, x_4) = 8x_1x_2x_3x_4$. From these relations it is easy to conjecture

Proposition A

$$F_n(x_1, x_2, \cdots, x_n) = 2^{n-1}x_1x_2\cdots x_n. \tag{6}$$

This is well-known [4], but I don't know the usual proof (in [4] there is no proof). This proof may be not easy for non-experts against the claim in the book [1], see pp. 30-31. Here let us introduce a new (?) method to prove this. For that we must make some mathematical preparations. First let us extend the operation $\oplus$ in Z_2 to an operation $\tilde{\oplus}$ in Z : for $x, y \in Z$

$$x\tilde{\oplus}y \equiv x + y - 2xy. \tag{7}$$

Of course $x\tilde{\oplus}y = x \oplus y$ for $x, y \in Z_2$. Here we list some important properties of this operation :

Lemma 1 For $x, y, z \in Z$

$$\begin{aligned} x\tilde{\oplus}y &= y\tilde{\oplus}x, \\ (x\tilde{\oplus}y)\tilde{\oplus}z &= x\tilde{\oplus}(y\tilde{\oplus}z), \\ x\tilde{\oplus}z + y\tilde{\oplus}z &= (x+y)\tilde{\oplus}z + z, \\ x\tilde{\oplus}z - y\tilde{\oplus}z &= (x-y)\tilde{\oplus}z - z \end{aligned} \tag{8}$$

We also note that $x\tilde{\oplus}0 = x,\ x\tilde{\oplus}1 = 1-x,\ x\tilde{\oplus}x = 2x(1-x)$.

What we want to prove in this section is the following recurrent relation

Proposition B For $x_1, \cdots, x_n, x_{n+1} \in Z_2$

$$F_{n+1}(x_1, \cdots, x_n, x_{n+1}) = F_n(x_1, \cdots, x_n) + x_{n+1} - F_n(x_1, \cdots, x_n)\tilde{\oplus}x_{n+1}. \tag{9}$$

If we can prove this , then it is easy to see from the definition of $\tilde{\oplus}$

$$F_{n+1}(x_1, \cdots, x_n, x_{n+1}) = 2x_{n+1}F_n(x_1, \cdots, x_n). \tag{10}$$

From this we have Proposition A. Before giving the proof to Proposition B we make some preliminaries.

Lemma 2 For $x_1, \cdots, x_n, z \in Z_2$

$$\sum_{i=1}^{n} x_i \oplus z = \left(\sum_{i=1}^{n} x_i\right)\tilde{\oplus}z + (n-1)z, \tag{11}$$

$$\sum_{i=1}^{n}(-1)^{i-1}x_i \oplus z = \left(\sum_{i=1}^{n}(-1)^{i-1}x_i\right)\tilde{\oplus}z - \frac{1+(-1)^n}{2}z. \tag{12}$$

The proof is straightforward from Lemma 1.

Lemma 3 For $n \geq 2$

$$\sum_{i=1}^{n-1}(-1)^i({}_nC_i - 1) = -\frac{1+(-1)^n}{2}. \tag{13}$$

The proof is as follows :

$$\begin{aligned}
\text{Left hand side} &= \sum_{i=1}^{n-1}(-1)^i{}_nC_i + \sum_{i=1}^{n-1}(-1)^{i+1} \\
&= \sum_{i=0}^{n}(-1)^i{}_nC_i - \{1+(-1)^n\} + \sum_{i=0}^{n-2}(-1)^i \\
&= (1-1)^n - \{1+(-1)^n\} + \frac{1-(-1)^{n-1}}{2} \\
&= -\{1+(-1)^n\} + \frac{1+(-1)^n}{2} \\
&= -\frac{1+(-1)^n}{2}. \quad \heartsuit
\end{aligned}$$

First of all let us show my idea to prove Proposition B with a simple example.

$$F_3(x_1, x_2, x_3) = x_1 + x_2 + x_3 - (x_1 \oplus x_2 + x_1 \oplus x_3 + x_2 \oplus x_3) + x_1 \oplus x_2 \oplus x_3$$

$$
\begin{aligned}
&= x_1 + x_2 - x_1 \oplus x_2 + x_3 - \{x_1 \oplus x_3 + x_2 \oplus x_3 - x_1 \oplus x_2 \oplus x_3\} \\
&= F_2(x_1, x_2) + x_3 - \left\{(x_1 + x_2)\tilde{\oplus} x_3 + x_3 - x_1 \oplus x_2 \oplus x_3\right\} \\
&= F_2(x_1, x_2) + x_3 - \left\{(x_1 + x_2 - x_1 \oplus x_2)\tilde{\oplus} x_3 - x_3 + x_3\right\} \\
&= F_2(x_1, x_2) + x_3 - F_2(x_1, x_2)\tilde{\oplus} x_3. \quad \heartsuit
\end{aligned}
$$

Let us start the proof of Proposition B.

$$
\begin{aligned}
F_{n+1}(x_1, \cdots, x_n, x_{n+1}) &= \sum_{i=1}^{n+1} x_i - \sum_{i<j}^{n+1} x_i \oplus x_j + \sum_{i<j<k}^{n+1} x_i \oplus x_j \oplus x_k - \cdots \\
&\quad +(-1)^{n-1} \sum_{i=1}^{n+1} x_1 \oplus \cdots \oplus \breve{x}_i \oplus \cdots \oplus x_{n+1} + (-1)^n x_1 \oplus \cdots \oplus x_n \oplus x_{n+1} \\
&= F_n(x_1, \cdots, x_n) + x_{n+1} - \sum_{i=1}^{n} x_i \oplus x_{n+1} + \sum_{i<j}^{n} x_i \oplus x_j \oplus x_{n+1} - \cdots \\
&\quad +(-1)^{n-1} \sum_{i=1}^{n} x_1 \oplus \cdots \oplus \breve{x}_i \oplus \cdots \oplus x_n \oplus x_{n+1} + (-1)^n x_1 \oplus \cdots \oplus x_n \oplus x_{n+1} \\
&= F_n(x_1, \cdots, x_n) + x_{n+1} \\
&\quad - \left\{ \left(\sum_{i=1}^{n} x_i \right) \tilde{\oplus} x_{n+1} + ({}_nC_1 - 1) x_{n+1} \right\} \\
&\quad + \left\{ \left(\sum_{i<j}^{n} x_i \oplus x_j \right) \tilde{\oplus} x_{n+1} + ({}_nC_2 - 1) x_{n+1} \right\} \\
&\quad \cdots \\
&\quad +(-1)^{n-1} \left\{ \left(\sum_{i=1}^{n} x_1 \oplus \cdots \oplus \breve{x}_i \oplus \cdots \oplus x_n \right) \tilde{\oplus} x_{n+1} + ({}_nC_{n-1} - 1) x_{n+1} \right\} \\
&\quad +(-1)^n x_1 \oplus \cdots \oplus x_n \oplus x_{n+1} \\
&= F_n(x_1, \cdots, x_n) + x_{n+1} - \left(\sum_{i=1}^{n} x_i \right) \tilde{\oplus} x_{n+1} + \left(\sum_{i<j}^{n} x_i \oplus x_j \right) \tilde{\oplus} x_{n+1} - \cdots \\
&\quad +(-1)^{n-1} \left(\sum_{i=1}^{n} x_1 \oplus \cdots \oplus \breve{x}_i \oplus \cdots \oplus x_n \right) \tilde{\oplus} x_{n+1} + (-1)^n x_1 \oplus \cdots \oplus x_n \oplus x_{n+1} \\
&\quad + \left\{ \sum_{i=1}^{n-1} (-1)^i ({}_nC_i - 1) \right\} x_{n+1} \\
&= F_n(x_1, \cdots, x_n) + x_{n+1} - \left\{ \sum_{i=1}^{n} x_i - \sum_{i<j}^{n} x_i \oplus x_j + \cdots \right. \\
&\quad \left. +(-1)^{n-2} \sum_{i=1}^{n} x_1 \oplus \cdots \oplus \breve{x}_i \oplus \cdots \oplus x_n + (-1)^{n-1} x_1 \oplus \cdots \oplus x_n \right\} \tilde{\oplus} x_{n+1} \\
&\quad + \frac{1 + (-1)^n}{2} x_{n+1} - \frac{1 + (-1)^n}{2} x_{n+1} \qquad \text{by Lemma 2 and Lemma 3}
\end{aligned}
$$

$$= \quad F_n(x_1, \cdots, x_n) + x_{n+1} - F_n(x_1, \cdots, x_n)\tilde{\oplus} x_{n+1}. \quad \heartsuit$$

One word : I introduced one method to prove Proposition A. Of course we have an another one [5], but in my teaching experience my method was popular among young graduate students.

3 General Controlled Unitary Gates

Let a basis of 1-qubit space $\boldsymbol{C}^2$ be $\{|0\rangle, |1\rangle\}$.,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and 2-qubit space $\boldsymbol{C}^2 \otimes \boldsymbol{C}^2$ be

$$\boldsymbol{C}^2 \otimes \boldsymbol{C}^2 = \mathrm{Vect}_C\{|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle\} \cong \boldsymbol{C}^4$$

where $|i,j\rangle \equiv |i\rangle \otimes |j\rangle$ for $i, j = 0, 1$.

The controlled NOT operation is defined as

$$\begin{aligned} \text{C-NOT} : \qquad & |0,0\rangle \to |0,0\rangle, \quad |0,1\rangle \to |0,1\rangle, \\ & |1,0\rangle \to |1,1\rangle, \quad |1,1\rangle \to |1,0\rangle \end{aligned} \tag{14}$$

and , therefore, the matrix representation is

$$\text{C-NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{15}$$

and represented graphically as

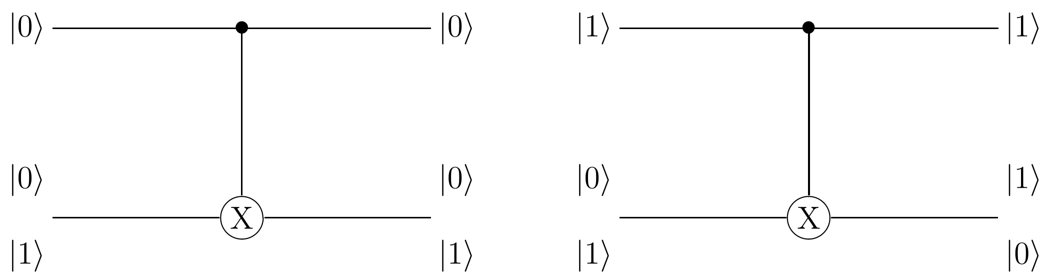

Figure 1

Let U be an arbitrarily unitary matrix in $U(2)$. Then the controlled unitary gates are defined as

$$\begin{aligned} \text{C-U}: \qquad & |0,0\rangle \to |0,0\rangle, \quad |0,1\rangle \to |0,1\rangle, \\ & |1\rangle \otimes |0\rangle \to |1\rangle \otimes (U|0\rangle), \quad |1\rangle \otimes |1\rangle \to |1\rangle \otimes (U|1\rangle) \end{aligned} \tag{16}$$

more briefly,

$$\text{C-U}: |x\rangle \otimes |y\rangle \to |x\rangle \otimes (U^x|y\rangle) \quad \text{for} \quad x, y \in Z_2 \tag{17}$$

and represented graphically as

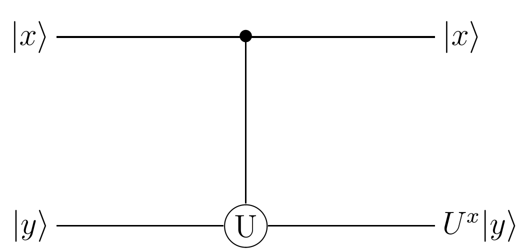

Figure 2

If $U = \sigma_2 = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then the controlled unitary gate is just controlled NOT gate. The controlled-controlled unitary gates are defined as

$$\text{C-C-U}: |x\rangle \otimes |y\rangle \otimes |z\rangle \to |x\rangle \otimes |y\rangle \otimes (U^{xy}|z\rangle) \quad \text{for} \quad x, y, z \in Z_2. \tag{18}$$

The controlled-controlled unitary gates are constructed by making use of several controlled unitary gates and controlled NOT gates : Let U be an arbitrarily unitary matrix in $U(2)$ and V a unitary one in $U(2)$ satisfying $V^2 = U$. Then by relation (2)

$$V^{x+y-x\oplus y} = V^{2xy} = (V^2)^{xy} = U^{xy}, \tag{19}$$

controlled-controlled U gate is graphically represented as

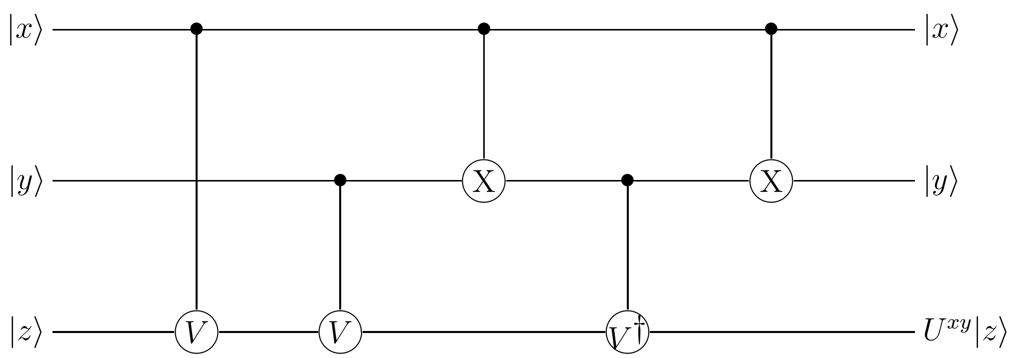

Figure 3

The controlled-controlled-controlled unitary gates are constructed by the following : Let U be an arbitrarily unitary matrix in $U(2)$ and V be a unitary one in $U(2)$ satisfying $V^4 = U$. Then making use of (3)

$$V^{x+y+z-(x\oplus y+x\oplus z+y\oplus z)+x\oplus y\oplus z} = V^{4xyx} = U^{xyz}, \tag{20}$$

controlled-controlled-controlled U gate is graphically represented as

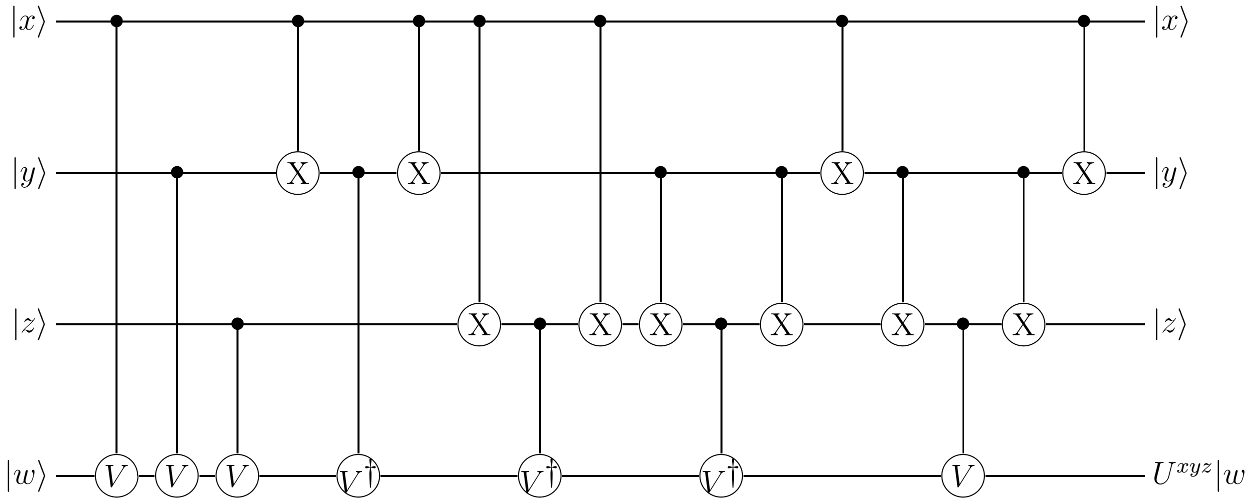

Figure 4

The general controlled unitary gates are constructed by the following : Let U be an arbitrarily unitary matrix in $U(2)$ and V be a unitary one in $U(2)$ satisfying $V^{2^{n-1}} = U$. Then making use of relation (6)

$$V^{F_n(x_1,x_2,\cdots,x_n)} = V^{2^{n-1}x_1x_2\cdots x_n} = U^{x_1x_2\cdots x_n}, \tag{21}$$

the construction of n-repeated controlled U gate is as follows : For example the block implementing $V^{x_i \oplus x_j \oplus x_k}$ is graphically constructed as

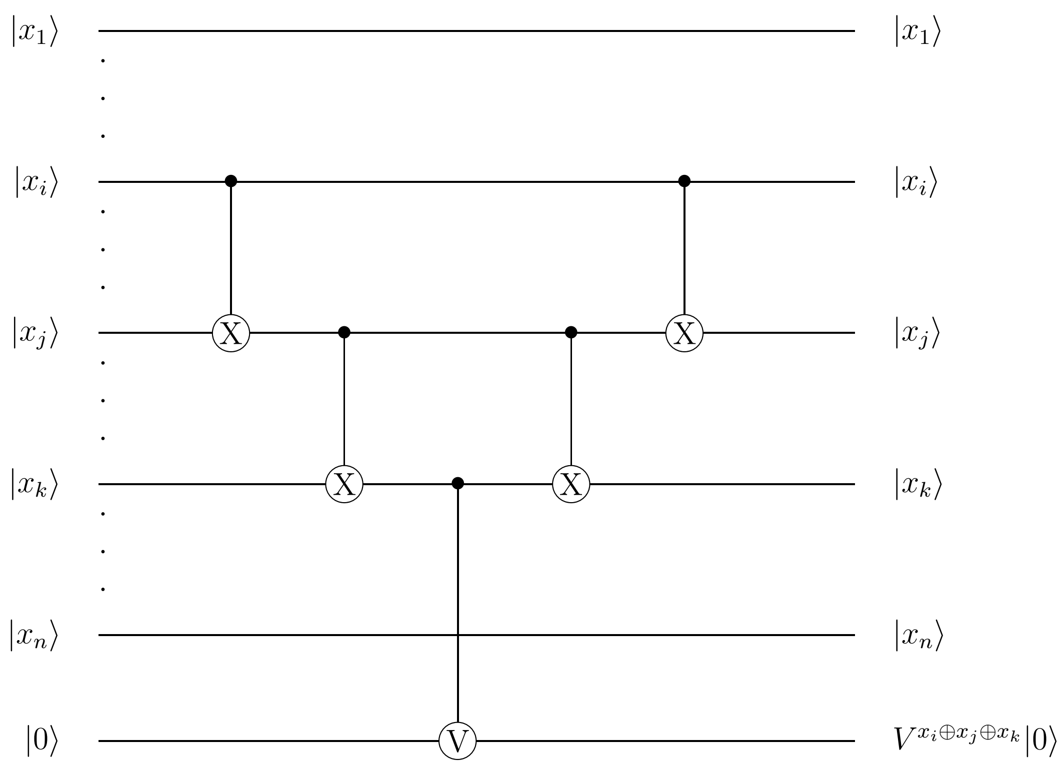

Figure 5

By combining these blocks like Figure 3 and Figure 4 we have the n-repeated controlled unitary gates. But as emphasized in [4] this construction is not efficient.

Acknowledgment. The author wishes to thank Michiko Kasai for tex-typing of several figures and Tatsuo Suzuki for helpful suggestions.

References

[1] A. Hosoya : Lectures on Quantum Computation (in Japanese), 1999, Science Company (in Japan).

[2] A. Steane : Quantum Computing, Rept. Prog. Phys. 61, 117, 1998, quant-ph/9708022.

[3] E.Rieffel and W. Polak : An Introduction to Quantum Computing for Non-Physicists, quant-ph/9809016.

[4] A. Barenco, C. H. Bennett, R. Cleve, D. P. Vincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter : Elementary gates for quantum computation, Phys. Rev. A 52, 3457, 1995, quant-ph/9503016.

[5] T. Suzuki : a private communication.